

## UNITED STATES DISTRICT COURT

for the  
Northern District of New York

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

THE SNAPCHAT ACCOUNT "LUCIFERJAMES12"  
THAT IS STORED AT PREMISES CONTROLLED BY  
SNAP, INC.

Case No. 1:25-sw-86-2 (PJE)

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Central District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

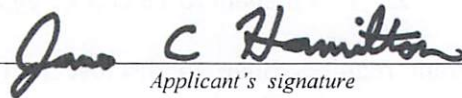
Offense Description

18 U.S.C. § 2252A(a)(1), (a)(2) Transportation of child pornography, distribution and receipt of child pornography,  
(A), (a)(5)(B) possession or knowing access with intent to view child pornography

The application is based on these facts:

See affidavit

- ☐ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Special Agent James C. Hamilton  
Printed name and title

Sworn to before me and signed in my presence.

Date: 4/11/2025

City and state: Albany, NY

  
Judge's signature

Magistrate Judge Paul J. Evangelista  
Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF  
THE SNAPCHAT ACCOUNT  
“LUCIFERJAMES12” THAT IS STORED AT  
PREMISES CONTROLLED BY SNAP, INC.

Case No. 1:25-sw- 86-2(PJE)

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, **James Hamilton**, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) for a warrant to search information associated with the following account assigned Snapchat Username luciferjames12 (the “SUBJECT ACCOUNT”), maintained by Snap, Inc. (“Snap”), which is stored at premises owned, maintained, controlled, or operated by Snap, a company headquartered at 2772 Donald Douglas Loop North, Santa Monica, CA 90405. Located within the SUBJECT ACCOUNT to be searched, as more particularly described in Attachment A, I seek to seize evidence and instrumentalities relating to violations of Title 18, United States Code, Sections 2252A(a)(1) (transportation of child pornography), (a)(2)(A) (distribution and receipt of child pornography), and (a)(5)(B) (possession or knowing access with intent to view child pornography) (the “SUBJECT CRIMES”), as more fully described in Attachment B.

2. Pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), the proposed warrant requires Snap to disclose to the government copies of the records, data and other information (including the content of communications, if available) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment

B, government agents will review that information to locate the items described in Section II of Attachment B.

3. I am a Special Agent with the U.S. Immigration and Customs Enforcement Office of Homeland Security Investigations (“HSI”) and have been since June 2002. As such, I am an investigative or law enforcement officer of the United States within the meaning of Title 18 United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516(1). I have been a law enforcement officer for 28 years. I was a police officer for approximately 5 years and have been a Special Agent for 23 years. My career as a Special Agent began in June 2002 with the U.S. Customs Service, which is now known as U.S. Immigration and Customs Enforcement Homeland Security Investigations (HSI). Prior to my employment as a Special Agent, I was a police officer in the state of Tennessee from September 1997 until June 2002.

4. As an HSI Special Agent, I am authorized to seek and execute federal arrest and search warrants for Title 18 criminal offenses, including offenses related to the sexual exploitation of minors, specifically those involving the sexual exploitation of children, in violation of Title 18, United States Code, Section 2251(a), and involving the possession, distribution, and receipt of child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I have a Bachelor of Science Criminal Justice degree and a Master of Public Management degree. I have completed the Criminal Investigator Training Program and Customs Basic Enforcement School at the Federal Law Enforcement Training Center in Glynco, GA. During both basic training, and subsequent training, I received instruction on conducting online child pornography investigations.

I have also been the affiant for and participated in the execution of numerous Federal search warrants in child pornography and child exploitation investigations.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2252A(a)(1) (transportation of child pornography), (a)(2)(A) (distribution and receipt of child pornography), and (a)(5)(B) (possession or knowing access with intent to view child pornography) have been committed, and that evidence of these crimes and contraband or fruits of those crimes, as described in Attachment B, exist within said SUBJECT ACCOUNT which is stored at premises owned, maintained, controlled, or operated by Snap.

### **JURISDICTION**

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **BACKGROUND ON SNAPCHAT<sup>1</sup>**

8. Snapchat is a service owned and made by Snap, Inc., a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510.

---

<sup>1</sup> The information in this section is based on information published by Snap on its website, including, but not limited to, the following webpages: “Privacy Policy,” <https://www.snap.com/en-US/privacy/privacy-policy> ; “Snap Inc. Law Enforcement Guide,” <https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf> and “Snapchat Support,” <https://support.snapchat.com/en-US>.

Snapchat is a free-access social networking application, accessible through its website and its mobile application, that allows subscribers to acquire and use Snapchat accounts, like the SUBJECT ACCOUNT, through which users can share messages, multimedia (including photos and videos), and other information with other Snapchat users and the general public. The mobile application is available through the iPhone App Store and Google Play.

9. Snapchat's differentiating feature from other communications applications is that a sender is able to set a variable amount of time (between one and ten seconds) that a recipient can view a message. At the expiration of that time, the message is deleted from Snapchat's servers. Similarly, the message disappears from the user's devices. If the receiver of a Snapchat message does not access the application on their device the message remains undelivered. Snapchat stores undelivered messages for 30 days. After 30 days the messages are deleted from the company's servers.

10. Snapchat users have the following abilities:

- a. **Snap:** A user takes a photo or video using their camera phone in real-time and then selects which of their friends to send the message to. Pictures and videos can also be sent from the saved pictures/videos in the gallery of the device. Unless the sender or recipient opts to save the photo or video, the message will be deleted from their devices (after the content is sent in the case of the sender and after it's opened in the case of the recipient). Users are able to save a photo or video they've taken locally to their device or to Memories, which is Snapchat's cloud-storage service.
- b. **Stories:** A user can add photo or video snaps to their "Story." Depending on the user's privacy settings, the photos and videos added to a Story can be viewed by either all Snap chatters or just the user's friends for up to 24 hours. Stories can also

be saved in Memories. Our Stories is a collection of user-submitted snaps from different locations and events. A Snapchat user, with the location services of their device turned on, can contribute to a collection of snaps regarding the event.

- c. **Memories:** Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. A user can also edit and send Snaps and create Stories from these Memories. Snaps, Stories, and other photos and videos saved in Memories are backed up by Snapchat and may remain in Memories until deleted by the user.
- d. **Chat:** A user can also type messages, send photos, videos, audio notes, and video notes to friends within the Snapchat app using the Chat feature. A user sends a Chat message to a friend, and once it is viewed by both parties – and both parties swipe away from the Chat screen – the message will be cleared. Within the Snapchat app itself, a user can opt to save part of the Chat by tapping on the message that they want to keep. The user can clear the message by tapping it again.
- e. **Snapcash:** Snapchat also offers a money transfer service called Snapcash. Users are able to transfer up to \$2,500 per week using this service. Snapcash transactions are only permitted using Visa and Mastercard debit cards issued by a United States Financial Institution. Money transfers can only occur if the sender and receiver both have Snapchat installed and have linked an appropriate debit card to their accounts. To facilitate this transaction, Snapchat retains information about the method and source of payment including debit card information such as the card number, expiration date, CVV security code, and billing address zip code.



Additionally, the company may have the date of birth and social security number of those involved in money transfers.

11. Snap possesses and maintains the following information:
  - a. Personally-Identifying Information: When a user creates an account they make a unique Snapchat username. This is the name visible to other Snapchat users. A user also enters a data of birth. This is supposed to prevent anyone under the age of 13 from using Snapchat. An email address is required to register a Snapchat account. A new user also has to provide a mobile phone number. This phone number is verified during the registration process. Snapchat sends an activation code that must be entered before proceeding with the registration step. However, a user may elect to bypass entering a phone number so one may not always be present in the user's account. Snapchat also retains the account creation date.
  - b. Usage Information: While a Snapchat message may disappear, the record of who sent it and when still exists. Snapchat records and retains log files and information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.
  - c. Device Information: Snapchat stores device information such as the model, operating system, operating system version, mobile device phone number, and mobile network information of devices used in conjunction with the service. They

also collect unique device identifiers such as the Media Access Control (MAC) address and the International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of devices used to access Snapchat.

- d. **Device Phonebook and Photos:** If a user consents, Snapchat can access from their device's electronic phonebook or contacts list and images.
- e. **Financial information:** Snapchat retains information about the method and source of payment of customers who use the Snapcash service. This includes debit card information such as the card number, expiration date, CVV security code, and billing address zip code. Additionally, the company may have the date of birth and social security number of those involved in money transfers. Snapcash generate a receipt for any transaction. The receipts are programmed to automatically delete after the sender and recipient have seen the message and swiped out of the Chat screen, unless taps to save the message. Snapchat maintains transactional records for ten days. These records include information about the sender and receiver, the transaction amount, and date/time stamps of when the message was sent, received, and opened.
- f. **Message Content:** Snapchat's motto is 'delete is our default.' Snapchat deletes a snap once it has been viewed. If the message is not read, because the user has not opened up the application, the message is stored for 30 days before being deleted. However, just because the snap no longer appear to the user, it doesn't necessarily mean it is gone. For example, Snapchat has a feature called Replay. This allows users to view a previously viewed snap once per day. This feature is disabled by default and the user must opt-in to use Replay. Also, if a Snapchat user posts an



image or video to the MyStory feature it can be viewed by their friends for 24 hours.

If the user posted to the Our Stories feature, the snaps are archived and can be viewed through Snapchat.

- g. Location Data: If a user has device-level location services turned on and has opted into location services on Snapchat, Snap will collect location data at various points during the user's use of Snapchat, and retention periods for location data vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the app settings.

12. Snap collects basic contact and personal identifying information from users during the Snapchat registration process. This information, which can later be changed by the user, may include the user's Snapchat username, contact e-mail addresses, telephone numbers, and other personal identifiers. Snap keeps records of changes made to this information.

13. Snap also collects and retains information about how each user accesses and uses Snapchat. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations. This also includes information about a user's hardware and software, such as the hardware model, operating system version, device memory, advertising identifiers, unique application identifiers, apps installed, unique device identifiers, device usage data, browser type, keyboards installed, language, battery level, and time zone.

14. Each Snapchat account is identified by a unique username. A Snapchat username is a unique identifier associated with a specific Snapchat account, and it cannot be changed by the user. A Snapchat display name, on the other hand, is not a unique identifier and can be created and

changed by a user to indicate how the user will appear within the app. A user can also change a friend's display name to determine how that friend will appear to that particular user on the app, similar to how one can customize contact names on a smartphone. If a display name has not been created, the username will appear on its own

15. Users have several ways to search for friends and associates to follow on Snapchat, such as by allowing Snap to access the contact lists on their devices to identify which contacts are Snapchat users. Snap retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can also manually search for friends or associates.

16. Snap collects and retains location information relating to the use of a Snapchat account, including how users interact with Snap's services, such as which Filters or Lenses are viewed or applied to Snaps, which Stories are watched, and which search queries a user submits. Snap also collects information about how users communicate with other Snapchatters, such as their names, the time and date of your communications, the number of messages exchanged, which friends exchange messages with the most other users, and a user's interactions with messages (such as when a message is opened, or a screenshot is captured).

17. Snap uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

18. In some cases, Snapchat users may communicate directly with Snap about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Snap typically retain records about such communications,

including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

19. For each Snapchat user, Snap collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

20. In my training and experience, evidence of who was using Snapchat and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

21. This investigation concerns the transportation, receipt, distribution, and possession of child pornography using social media, including Snapchat. The investigation has revealed that a Snapchat account, believed to be used, owned, and controlled by Conner BUSKEY, has communicated via that Snapchat account, where he may have shared media files as well as chats. For example, the stored communications and files connected to a Snapchat account may provide direct evidence of the offenses under investigation by revealing the person controlling the account and evidence of the child pornography sent and received using that account. Based on my training and experience, instant messages, voice messages, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

22. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Snap can indicate who has used or controlled the account. This "user

attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, messaging logs, photos, and videos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

23. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

24. Other information connected to the use of Snapchat may lead to the discovery of additional evidence. For example, associated and linked accounts, stored communications, photos, and videos may reveal services used in furtherance of the crimes under investigation or services used to communicate with other individuals engaged in the sexual exploitation of children. For example, another social media or communications app may indicate other methods of communication between individuals engaged in exploiting children, and other repositories of stored communications. Accordingly, stored communications, contact lists, photos, and videos can lead to the identification of contraband and other accounts and instrumentalities of the crimes under investigation.

25. Therefore, Snap's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Snapchat. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

**BACKGROUND INFORMATION ABOUT THE NCMEC CYBERTIPLINE**

26. The National Center for Missing & Exploited Children or NCMEC is a private, nonprofit corporation based in the United States. It was created to help find missing children, reduce child sexual exploitation, and prevent child victimization. NCMEC serves as the national clearinghouse for families, victims, private industry, law enforcement, and other professionals on information and programs related to missing and exploited children's issues. NCMEC employs more than 330 individuals and works with hundreds of volunteers to facilitate outreach and community child safety events nationwide.

27. NCMEC began operating the CyberTipline on March 9, 1998, to serve as the national online clearinghouse for tips and leads relating to instances of child sexual exploitation. The CyberTipline ([www.missingkids.org/cybertipline](http://www.missingkids.org/cybertipline)) was developed to further NCMEC's private mission to help prevent and diminish the sexual exploitation of children by allowing the public and electronic service providers (ESPs) to report online (and via toll-free telephone) the enticement of children for sexual acts, extra-familial child sexual molestation, child pornography, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, misleading words or digital images on the Internet. A secure CyberTipline was created in February 2000 to facilitate the reporting of apparent child pornography by ESPs. Once registered with NCMEC, ESPs can upload files relating to child sexual exploitation content when

making reports to NCMEC using a secure electronic connection. Uploaded files may include images, video, or other reported content.

28. Neither the government nor any law enforcement agency created the CyberTipline or has input into CyberTipline operations. The government does not instigate, direct, or provide guidance to NCMEC in its processing of CyberTipline reports. NCMEC receives complaints via their CyberTipline from Internet Service Providers (ISPs), ESPs, and others. These CyberTipline reports are reviewed by a NCMEC analyst and forwarded to law enforcement for further investigation based on the information provided in the CyberTipline report.

29. CyberTipline Reports, also referred to as CyberTip reports, are provided directly to HSI through an HSI Special Agent, who is assigned to NCMEC as the HSI liaison. The reports are then directed to the appropriate HSI field office through the HSI liaison. NCMEC also provides CyberTip reports to other federal law enforcement agencies and to state and local agencies through Internet Crimes Against Children (ICAC) Task Forces in every state. In New York, there are two ICAC Task Forces, one operated by the New York City Police Department and the other operated by the New York State Police. The CyberTip report referenced in this search warrant affidavit were provided to your affiant after being received at the New York ICAC Task Force located in Albany, New York.

**PROBABLE CAUSE**

**CyberTip Report 205186799**

17. On or about January 22, 2025, NCMEC received information reported by Snapchat, in which Snapchat reported that one child pornography video file was uploaded when the “user shared this media file in chat” from the Snapchat user account luciferjames12, the SUBJECT ACCOUNT. The information received by NCMEC resulted in the issuance of CyberTip Report



205186799. In that CyberTip report, for the reported file, the question is asked, “Did Reporting ESP view entire contents of uploaded file?” and Snapchat answered “Yes.” A second question is asked “Were the entire contents of the uploaded file publicly available?” and Snapchat answered “Yes.” The file reported by Snapchat to NCMEC is described as follows:

a. Filename: 1:2cb633fe-0285-55b7-b382-eac630d8ebec:33:0:0~web.mp4, MD5: 32e994af431891a7794e8a271d294a3c, is an 11-second video file that depicts a naked prepubescent female bent backwards, on her hands and feet. The camera is in front of the girl and is focused on the anus and vagina of the girl. The girl’s right hand is touching her vagina. The age of the girl appears to be approximately 8-11 years old. The CyberTip report states that 2025-01-22T05:22:18.858Z is the timestamp when the user shared this media file in a chat.

18. In addition to reporting child pornography video file that was shared from the SUBJECT ACCOUNT, Snapchat also reported the chat conversation that occurred between luciferjames12 and the user of a second Snapchat account just prior to the sharing of the child pornography video file. The following is the chat conversation that was reported:

- a. luciferjames12 (Reported) 2025-01-22T05:17:59.120Z: Does ur friend have lmk
- b. ACCOUNT 2 (REDACTED) 2025-01-22T05:18:16.017Z: Oh idk where are friends in really life
- c. ACCOUNT 2 (REDACTED) 2025-01-22T05:18:19.907Z: Real\*
- d. luciferjames12 (Reported) 2025-01-22T05:18:57.770Z: Well I was gunna start a room on lmk
- e. ACCOUNT 2 (REDACTED) 2025-01-22T05:19:22.344Z: U have fun on there 🤔 I hate that stuff
- f. luciferjames12 (Reported) 2025-01-22T05:19:35.799Z: Why
- g. ACCOUNT 2 (REDACTED) 2025-01-22T05:20:30.209Z: I dont like to like talk talk to strangers
- h. luciferjames12 (Reported) 2025-01-22T05:20:45.286Z: Oh is someone shy
- i. ACCOUNT 2 (REDACTED) 2025-01-22T05:20:59.435Z: A little bit
- j. luciferjames12 (Reported) 2025-01-22T05:22:18.858Z: 1:2cb633fe-0285-55b7-b382-eac630d8ebec:33:0:0~web.mp4



19. Based on my training and experience, as well as a Google internet search and an Apple App Store search, I believe that that “lmk” refers to LMK, a messaging platform that advertises itself as LMK: Make New Friends. A “room” in social media applications generally refers to a space that can be created so that like-minded users can communicate.

20. Accordingly, there is probable cause to believe that the SUBJECT ACCOUNT contains child pornography files and was used to transport and distribute at least one file.

21. CyberTip Report 205186799 also contains a section titled “Incident Information.” The incident information is described as follows:

- a. Primary Incident Type: Child Pornography (possession, manufacture, and distribution)
- b. Incident Time: 01-22-2025 05:22:18 UTC
- c. Description of Incident Time: The Incident Date Time value is when the most recent media file being reported was saved, shared, or uploaded by the reported user.

22. Contained within CyberTip Report 205186799 is a section titled “Suspect.” The Suspect information is described as follows:

Date of Birth: 01-20-2003  
Email Address: stoneysyoung867@gmail.com (Verified 01-20-2025 18:19:28 UTC)  
Screen/Username: luciferjames12  
IP Address: 24.194.229.111 (Login) 01-22-2025 05:28:48 UTC  
IP Address: 24.194.229.111 (Other) 01-22-2025 05:28:33 UTC  
IP Address: 24.194.229.111 (Registration) 01-20-2025 18:14:35 UTC  
Additional Information: IP address data identified as “other” may be associated with one of several sources, including  
logout or app authentication events  
The account identifier provided is a “username” which should be provided when seeking data.  
The reported account has no phone number available.

23. On March 12, 2025, NCMEC provided CyberTip Report 205186799 to the New York Internet Crimes Against Children (ICAC) Task Force in Albany, New York, and it was assigned to New York State Police Investigator Meghan Lohman on the same date.

24. On or about March 18, 2025, a Department of Homeland Security (DHS) administrative summons was served to Charter Communications for subscriber information for IP address 24.194.229.111, used on 1/22/2025 at 5:28:48 AM UTC. This IP address is a SUBJECT ACCOUNT login IP address provided by Snapchat in CyberTip report 205186799, which occurred just after the sharing of the child pornography video file. Charter Communications responded on March 24, 2025, with the following subscriber information:

Subscriber Name: RXXXXXX PXXX (REDACTED)  
Service Address: 372 DANIELS RD BLDG 2, SARATOGA SPRINGS, NY 128669187  
Billing Address:  
Username or Features: DXXXXXXXXXXXX4@XXXXXXX.NET, CXXXXXXXXX0@XXXXX.COM (REDACTED)  
Phone number: 518XXXXX57 (REDACTED)  
Lease Log: Start Date: 01/13/2025 08:32 PM  
End Date: 03/20/2025 11:05 AM

The Lease Log start and end dates cover the entire activity of the time the SUBJECT ACCOUNT was active, from the registration date of January 20, 2025, through the upload date of January 22, 2025.

25. On or about April 1, 2025, Saratoga County New York Sheriff's Investigator Anthony Pirrone, who is also a HSI Task Force Officer, is conducting an investigation in which he arrested Conner BUSKEY, DOB XX/XX/2005 (REDACTED) and charged him with Rape In The First Degree in violation of New York Penal Law Section 130.35, Subsection 01A, for the rape of a child under the age of 13 that occurred on March 9, 2025. The rape occurred at BUSKEY's residence, 372 Daniels Road, Saratoga Springs, New York – the same address as the

subscriber of the IP address used to upload the child pornography file in the Snapchat SUBJECT ACCOUNT. I learned about this CyberTip investigation of the SUBJECT ACCOUNT after TFO Pirrone contacted the ICAC Task Force to inquire if BUSKEY's name or address is or was the target of any child pornography CyberTip investigations. After it was discovered that the suspect IP address for this CyberTip case matched the address of the alleged rape, Investigator Lohman turned over the ICAC investigation of the SUBJECT ACCOUNT to your affiant, and I am working with TFO Pirrone to further this investigation.

26. During his investigation of BUSKEY, TFO Pirrone, in his duties as a sheriff's investigator, read BUSKEY his "Miranda" rights, and after BUSKEY waived his Miranda rights, BUSKEY was interviewed. BUSKEY also gave written consent for TFO Pirrone to examine his cell phone. TFO Pirrone found deleted child pornography files on the phone, as well as user accounts on the phone. Of significance, on BUSKEY's cell phone was a user account for the email address [stoneysyoung867@gmail.com](mailto:stoneysyoung867@gmail.com), which was used on January 20, 2025, to verify the SUBJECT Snapchat ACCOUNT.

27. Based on the foregoing, there is probable cause to believe that violations of Title 18, United States Code, Sections 2252A(a)(1) (transportation of child pornography), (a)(2)(A) (distribution and receipt of child pornography), and (a)(5)(B) (possession or knowing access with intent to view child pornography) have been committed, and that evidence of these crimes and contraband or fruits of those crimes, as described in Attachment B, exist within said SUBJECT ACCOUNT which is stored at premises owned, maintained, controlled, or operated by Snap.

**CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTORS**

28. Based on my training, experience, and conversations with other law enforcement personnel, I am aware that the following characteristics are common to individuals involved in child pornography offenses:

- a. Individuals who use children for the purpose of producing sexually explicit material may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity, sexually suggestive poses, or from literature describing such activity.
- b. Individuals who use children for the purpose of producing sexually explicit material may collect sexually explicit or sexually suggestive material depicting children, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. These individuals often maintain this material for sexual arousal and gratification. Furthermore, they may use this material to lower the inhibitions of children they are attempting to seduce, to arouse a child partner, or to demonstrate the desired sexual acts.
- c. Individuals who use children for the purpose of producing sexually explicit material often possess and maintain copies of child pornographic material, including but not limited to pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, and tape recordings, in the privacy and security of their home. Prior investigations into these offenses have shown that child pornography offenders typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videos for many years.

- d. Individuals who use children for the purpose of producing sexually explicit material often begin their child pornography collections by obtaining child abuse material through various free avenues afforded by the Internet, like P2P file sharing. Thereafter, these individuals may escalate their activities by producing and/or distributing child pornography, for the purpose of trading this material to add to their own child pornography collection.
- e. Individuals who use children for the purpose of producing sexually explicit material often maintain their digital or electronic collections in a safe, secure and private environment, such as a computer or surrounding area. These collections are often maintained for several years and are maintained at the individual's residence or place of employment, to afford immediate access to view the material. These collections are often maintained for several years and are kept close by, usually at the individual's residence or sometimes vehicle, to enable the collector to view the collection, which is valued highly.
- f. Individuals who use children for the purpose of producing sexually explicit material may correspond with others to share information and material and rarely destroy this correspondence. These individuals often maintain lists of names, email addresses and telephone numbers of others with whom they have been in contact regarding their shared interests in child pornography.

\*\*\*\*

29. Based on all of the above, I believe that the SUBJECT ACCOUNT is a Snapchat account owned and controlled by Conner BUSKEY that remains active, and that BUSKEY used the Subject Account to send, receive, and possess child pornography. I

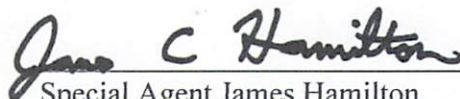
therefore believe that there is evidence of the SUBJECT CRIMES in the SUBJECT ACCOUNT.

**CONCLUSION**

30. Based on the forgoing, I request that the Court issue the proposed search warrant. I request that the warrant provide, notwithstanding 18 U.S.C. Sections 2252/2252A or any similar statutes or codes, that Snap Inc. disclose responsive data, if any, by sending it to Homeland Security Investigations, 11 Old Stonebreak Road, Malta, NY 12020, Attn: Special Agent James Hamilton, using the U.S. Postal Service or another courier service or electronic means to james.c.hamilton@hsi.dhs.gov.

31. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Snap. Because the warrant will be served on Snap, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Attested to by the affiant:



Special Agent James Hamilton  
Homeland Security Investigations

I, the Honorable Paul J. Evangelista, United States Magistrate Judge, hereby acknowledge that this affidavit was attested to by the affiant by telephone on April 11, 2025 in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.



Hon. Paul J. Evangelista  
United States Magistrate Judge

**ATTACHMENT A**

**Property To Be Searched**

This warrant applies to information associated with the Snapchat Username **luciferjames12** (the “SUBJECT ACCOUNT”), as reported in CyberTip Report 205186799, that is stored at premises owned, maintained, controlled, or operated by Snap Inc. (“Snap”), a company headquartered at 2772 Donald Douglas Loop North, Santa Monica, CA 90405.



**ATTACHMENT B**

**Particular Things To Be Seized**

**I. Information to be disclosed by Snap Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Snap, regardless of whether such information is located within or outside the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Snap, Snap is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- A. A copy of the files created and reported in CyberTip Report 205186799.
- B. All business records and subscriber information, in any form kept, pertaining to the account, including:
  - a. Snapchat username
  - b. Email address
  - c. Phone number
  - d. Display name
  - e. Snapchat account creation date and IP address
  - f. Timestamp and IP address of account logins and logouts
  - g. Device information and device history
  - h. Purchase history (information about services and items purchased through Snap, including in-app purchases, custom filters, and lenses -- includes what was purchased and date of purchase)

- i. Account change history (a log of changes to the account made by the user, including dates/times of changes in registration email address or phone number, birthdate, and display name)
  - j. Whether account phone number has been verified
  - k. Last active date
  - l. Whether Snap Map is enabled
  - m. Whether two-factor-authentication is enabled
  - n. App version; and
  - o. Communications between Snap and any person regarding the account, including contacts with support services and records of actions taken.
- C. All other Snapchat and third-party accounts that are linked to the SUBJECT ACCOUNT by cookies; recovery, secondary, forwarding, or alternate email address; telephone number, including SMS recovery number and sign-in account number; Android ID; IMEI; or creation IP address, provide the following information about the customers or subscribers of each linked account.
- D. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos, images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata;
- E. All content, records, and other information relating to communications sent from or received by the account, including but not limited to:

- a. The content of all communications sent from or received by the account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;
  - b. Memories content;
  - c. “Our Story” and Crowd-Sourced Content;
  - d. Snap History;
  - e. All records and other information about direct, group, and disappearing messages sent from or received by the account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);
  - f. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and
  - g. All associated logs and metadata, including logs containing metadata about a user’s Snaps, Stories, and Chats;
  - h. Additional user profile data, including number of Stories viewed; “discover channels” viewed; and ads, apps, and websites that the user has interacted with
  - i. Subscriptions (the accounts and/or “discover channels” to which a user has “subscribed”)
  - j. Friends (overview of the user’s friends, the friend requests sent, and users blocked and deleted)
- F. All content, records, and other information relating to all other interactions between the account and other Snapchat users, including but not limited to:

- a. Interactions by other Snapchat users with the account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;
  - b. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;
  - c. All contacts and related sync information; and
  - d. All associated logs and metadata;
- G. All records of searches and Snap survey responses/results performed by the account; and
- H. All location information, including location history, login activity, information geotags, and related metadata.

Snap is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I, that constitutes evidence, contraband, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1) (transportation of child pornography), (a)(2)(A) (distribution and receipt of child pornography), and (a)(5)(B) (possession or knowing access with intent to view child pornography) (the “SUBJECT CRIMES”), involving the SUBJECT ACCOUNT, and Snapchat user **luciferjames12**, including for each identifier listed in Attachment A, information pertaining to the following matters:

- a. Any and all child pornography, and any and all visual depictions of minors engaging in sexually explicit conduct, as those terms are defined in Title 18, United States Code, Section 2256.
- b. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).
- c. Images, videos and other files depicting minors communicating with adults and/or adults professing to be minors.
- d. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, and notes, that display a sexual interest in minors.
- e. Evidence indicating the SUBJECT ACCOUNT owner’s state of mind as it relates to the crimes under investigation.
- f. The identity of the person(s) who created or used the SUBJECT ACCOUNT, including records that help reveal the whereabouts of such person(s).

- g. Communications or records regarding the sexual exploitation of minors.
- h. Correspondence and records regarding possessing, receiving, downloading, or distributing child pornography, including chat logs, electronic messages, ledgers, and records of communications with other individuals, including on any group or Snapchat story related to the exploitation of minors.
- i. Communication or records regarding the user providing their location to others.
- j. Any records or logs pertaining to IP address 24.194.229.111;
- k. All images, messages, videos, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of the SUBJECT CRIMES;
- l. Communication, information, documentation, and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;
- m. Evidence of the times the SUBJECT ACCOUNT was used;
- n. All images, messages and communications regarding wiping software, encryption, or other methods to avoid detection by law enforcement;
- o. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A and other associated accounts;
- p. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the SUBJECT ACCOUNT; and
- q. Evidence reported in CyberTip Report 205186799.

### **III. Disclosure By Provider**

Snap shall disclose responsive data, if any, by sending it to Homeland Security Investigations, Attn: Special Agent James Hamilton, 11 Old Stonebreak Road, Malta, New York 12020 using the U.S. Postal Service or another courier service or electronic means to matthew.a.jones@associates.hsi.dhs.gov, notwithstanding 18 U.S.C. §§ 2252, 2252A, or other similar state laws.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents with the Department of Homeland Security, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, Homeland Security Investigations may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.